

**U.S. Department of Justice**

*United States Attorney  
Southern District of New York*

*The Silvio J. Mollo Building  
One Saint Andrew's Plaza  
New York, New York 10007*

February 22, 2024

**BY ECF**

Hon. Jesse M. Furman  
United States District Judge  
Southern District of New York  
Thurgood Marshall U.S. Courthouse  
40 Foley Square  
New York, New York 10007

**Re: *United States v. Joshua Adam Schulte*,  
S2/3 17 Cr. 548 (JMF)**

Dear Judge Furman:

On February 1, 2024, this Court sentenced Joshua Adam Schulte principally to a term of imprisonment of 40 years, which included a term of 80 months' imprisonment on Schulte's convictions of three counts of receiving, possessing, and transporting child pornography in violation of 18 U.S.C. § 2552A(a)(1), (2), and (5); and the forfeiture of all of the defendant's right, title, and interest in various computers and computer equipment. (D.E. 1124 (judgment); *see* Ex. A (preliminary order of forfeiture)). The Court directed the defendant to file any objections to the forfeiture within two weeks, and on February 15, 2024, the defendant objected to the forfeiture of all computer equipment except his desktop computer and four external hard drives. (D.E. 1129).

**I. Background**

On March 15, 2017, special agents and other personnel with the Federal Bureau of Investigation ("FBI") conducted a search of Schulte's Manhattan apartment pursuant to a search warrant. In the course of that search, the FBI recovered dozens of computers, computer equipment, hard drives and other storage devices, cellphones, and other electronics equipment. That evidence included three computer towers, a server rack with two servers, a Samsung tablet computer, 10 external hard drives, 12 thumb drives, four cell phones, and a SIM card, as well as various MP3 players, a Kindle, two Xboxes, a digital camera, a Garmin navigation device, and over 100 CDs and DVDs.

In searching the computer that Schulte used as his primary desktop (the "Desktop"), which is item 1 on the Preliminary Order of Forfeiture, the FBI discovered thousands of images and videos containing child sex abuse materials ("CSAM") constituting child pornography under 18 U.S.C. § 2256(8) and thousands of additional images and videos containing child erotica. These files were stored in multiple encrypted locations on the Desktop, including within an encrypted

virtual machine (“VM”). *See, e.g.*, GX2301<sup>1</sup> at 2-26, 43-55; GX2302 at 2-3, 13-15, 20-31, 37-56, 110-26; Tr. 121-41, 158-68.

Schulte built the Desktop himself while employed at the Central Intelligence Agency (“CIA”) and brought it, and the CSAM it contained, to New York when he moved in late 2016. *See* Tr. 76-78. The Desktop’s internal hard drives were wiped on or about May 5, 2016, when Schulte sought to destroy evidence of his theft and transmission of classified national defense information from the CIA. *See* 2022 Tr. 1174-77. The VM with Schulte’s CSAM was created before the Desktop was wiped, and transferred onto the Desktop after the wipe. *See* Tr. 267-72, GX2302 at 70-74. The forensic evidence, similarly, shows that Schulte collected CSAM, both before and after the Desktop was wiped. *See, e.g.*, GX481. *See also generally* PSR ¶¶ 84-89.

Schulte used TOR, an encrypted, anonymous browser capable of accessing the dark web, to search for and download CSAM, *see* Tr. 140, 148-49, 152-54, 222-26; and also used Tails, an “amnesiac” operating system that is capable of booting from a thumb drive or external storage device and which automatically uses TOR for internet access. *See* 2022 Tr. 1106-11. Schulte also used secure data deletion tools like Eraser Portable, which also runs from a thumb drive, and Darik’s Boot And Nuke. 2022 Tr. 1115-20, 1122-25, 1167.

While detained pending trial, Schulte was provided with a laptop to review unclassified discovery and electronic copies of unclassified discovery maintained on various discs and external hard drives. Schulte was also granted regular visits to the Sensitive Compartmented Information Facility (“SCIF”) at the Courthouse to review classified discovery, as well as discovery containing CSAM. As the Court is aware, Schulte abused his SCIF access by using a smuggled thumb drive to transfer CSAM to his discovery review laptop, and to view that CSAM while at the Metropolitan Detention Center. *See* PSR ¶ 90; *see also* D.E. 954 (October 6, 2022 letter) & 1048 (May 24, 2023 letter).

Pursuant to search warrants issued in July, September, and October, 2022, Schulte’s discovery laptop, electronic devices that Schulte had access to in the SCIF (including a thumb drive), and Schulte’s discovery hard drives and other electronic media held at the MDC. In its review of these materials, the FBI discovered, in addition to evidence of Schulte’s copying and viewing CSAM materials, a large encrypted partition on the discovery laptop, as well as encrypted partitions on all four discovery hard drives Schulte had access to at the MDC. None of those devices had encrypted partitions when they were provided to Schulte.

## II. The Subject Properties

The Subject Properties, in addition to the Desktop, consist of computers, electronic devices, and portable storage devices recovered during the search of Schulte’s Manhattan apartment. An index of the electronic devices recovered from that search, including the Subject Properties, is annexed hereto.

---

<sup>1</sup> References to “GX” are to Government exhibits introduced at the 2023 trial; “Tr.” are to the transcript of proceedings at the 2023 trial; “2022 GX” are to Government exhibits introduced at the 2022 trial; and “2022 Tr.” are to Government exhibits introduced at the 2022 trial.

Subject Property number 7 is a second computer tower recovered from Schulte's apartment. *See* Tr. 79; GX127 & GX114. Schulte described this computer in an interview with the FBI and the U.S. Attorney's Office as a computer he also had built while employed at the CIA, and that he and a former roommate "played around with virtualization" on that computer. *See* Ex. A at 2.

Subject Property number 6 is a Samsung cellphone that was recovered from Schulte's apartment, *see* Tr. 83-84, GX112, GX2000, GX2002, & GX2401; and which contained passwords that Schulte used on the encrypted portions of the Desktop that stored CSAM, among other uses. *See* Tr. 213-15, 217-19. Subject Properties numbered 20, 21, and 22 are additional cellphones recovered from Schulte's apartment.

Subject Properties numbers 8 through 19 are external hard drives that were recovered from Schulte's apartment. Subject Property numbers 10, 11, 12, 13, 15, 17, 18, and 19, in particular, had been wiped—not simply reformatted, but securely wiped to remove all digital evidence stored on them, just as the Desktop had been. 2022 Tr. 1168-69; *see also* 2022 GX1704 at 103 (marked for identification).

Subject Properties numbers 2 and 23 through 27 are thumb drives recovered from Schulte's apartment. Subject Property number 5 is a Samsung Tablet recovered from Schulte's apartment. Subject Properties numbers 30 and 31 are SD cards recovered from Schulte's apartment. Subject Property number 32 is an AT&T SIM card recovered from Schulte's apartment.<sup>2</sup>

### III. Discussion

Pursuant to 18 U.S.C. § 2253, a person convicted of an offense under § 2252A shall forfeit, *inter alia*, "any property, real or personal, used or intended to be used to commit or to promote the commission of such offense or any property traceable to such property." 18 U.S.C. § 2553(a)(3). Forfeiture is a "part of the sentencing process," and "the government need prove facts supporting forfeiture only by a preponderance of the evidence." *United States v. Gaskin*, 364 F.3d 438, 421-62 (2d Cir. 2004).

Schulte does not contest the forfeiture of Subject Properties numbers 1 and 10 through 13. The evidence demonstrates by a preponderance, however, that the remaining properties were involved in Schulte's offenses, including the Subject Properties on which no CSAM has been identified. As an initial matter, the evidence shows that the Desktop is not the only computer equipment Schulte used to view, acquire, and store CSAM. The majority of Schulte's CSAM was found within a VM on the Desktop that was created on October 3, 2015, Tr. 268-72, GX2302 at 71-74; and copied onto the Desktop on May 5, 2016, after the Desktop was securely wiped. Tr. 267-68, GX2302 at 70, 2022 Tr. 1174-77. Schulte accessed online CSAM marketplaces using TOR before the VM was created, GX2302 at 34-36, and had numerous files containing CSAM

---

<sup>2</sup> Subject Properties numbers 3 and 4 are MP3 player devices. The Government withdraws its request for forfeiture of these two properties. The Government also is not seeking forfeiture of other electronic devices, including the Xboxes, Kindle, digital camera, Garmin, other MP3 players, CDs and DVDs, the server rack, and an additional computer tower.

and child erotica with modified and accessed dates prior to October 5, 2015. *See, e.g.*, GX481. And if the VM and encrypted “volume” container with Schulte’s CSAM were saved on the Desktop prior to his wiping that Desktop on May 5, 2016, they could only have been on the Desktop after May 5 if Schulte transferred the VM and the volume container to another computer or storage device prior to the wipe, and then re-transferred the files back to the Desktop. Thus, there is a preponderance of the evidence that Schulte viewed, downloaded, stored, and transported CSAM using electronic devices other than the Desktop.

Moreover, the evidence at the 2022 and 2023 trials, as well as evidence of Schulte’s abuse of computer equipment in prison, demonstrates Schulte’s rampant use of computers and storage media to commit crimes and to hide and to destroy evidence of those crimes. This includes:

- Schulte’s widespread use of virtualization and encryption to hide illegal materials and evidence of his acquiring, storing, and transferring illegal materials. Schulte stored child erotica and CSAM beneath several layers of encryption, and encrypted portions of his prison discovery laptop (another computer where he illegally downloaded and stored CSAM) and each of his discovery hard drives.
- Schulte’s use of secure data deletion tools, including Eraser Portable, described above, and Darik’s Boot And Nuke, a tool that securely wipes an entire hard drive.
- Schulte’s use of external storage devices to transport illegal materials, including CSAM. It is apparent that Schulte used external hard drives to illegally transport stolen classified materials from the CIA to his home, and then securely deleted data from the hard drives. It is also apparent that Schulte used a thumb drive to illegally transfer CSAM from the discovery hard drive in the courthouse SCIF to his discovery laptop, and used one or more external storage devices and/or computers to store CSAM at his home in Virginia.
- Schulte’s use of external storage devices for secure data deletion tools. As described above, Schulte used Eraser Portable, a thumb drive-based deletion tool. Schulte also used Tails, a thumb-drive of DVD bootable operating system that prevents records of the user’s activities from being saved on the host computer.
- Schulte’s intermingling of his espionage and CSAM offenses. Schulte used his courthouse SCIF access, intended for his review of classified discovery relating to the espionage charges, to illegally smuggle CSAM materials onto his discovery laptop. He then viewed those CSAM materials during the espionage trial. Similarly, Schulte repeatedly viewed CSAM on the Desktop during the time period he was researching secure file transfer methods and transferring the stolen CIA materials to WikiLeaks, and used the same Desktop and the same browser application (TOR) to commit the CSAM and offenses and to transmit the stolen CIA data.

Each of the Subject Properties is a type of device that Schulte has often and repeatedly used for illicit purposes, and many bear evidence of having been used in furtherance of criminal activity, including the Schulte’s use of encryption, virtualization, data wiping, and the use of external hard drives and thumb drives as transfer media and to hold tools for data hiding. Thus, there is a

preponderance of evidence with respect to each Subject Property that it was “used to commit or to promote the commission” of his child pornography offenses.

#### **IV. Conclusion**

For these reasons, the Government respectfully requests that the Court enter the Preliminary Order of Forfeiture with respect to each of the Subject Properties except item numbers 3 and 4.

Respectfully submitted,

DAMIAN WILLIAMS  
United States Attorney

by:                     /s/                      
Michael D. Lockard / Nicholas S. Bradley  
Assistant United States Attorneys  
(212) 637-2193 /-1581

cc: Defense counsel

Search Item No.	Evidence No.	Description	Subject Property No.
SC1	1B9	One (1) Black Tower-Imaged/Seized	1
SC2	1B10	One (1) SanDisk Thumb Drive - Seized	2
SC3	1B11	One (1) Logitech Mouse - Seized	n/a
SC4	1B12	One (1) SanDisk MP3 Player - Seized	3
SC5	1B13	One (1) SanDisk MP3 Player - Seized	4
SC6	1B14	One (1) Xbox 360s S/N: 033320322443 -Seized	n/a
SC7	1B15	One (1) Xbox 1 S/N: 149212254048 -Seized	n/a
SC8	1B16	One (1) Kindle (No S/N) - Seized	n/a
SC9	1B17	One (1) Samsung Tablet S/N: R52H60LF5RY -Seized	5
SC10	1B18	One (1) Kindle (No S/N) - Seized	n/a
SC11	1B19	One (1) Samsung Phone Model SM-J320P -Seized	6
SC12	1B20	One (1) Black Tower (No S/N) - Seized	7
SC13	1B21	One (1) 120 GB Samsung SSD S19HNSAD5517655 - Seized	8
SC14	1B22	One (1) Kingston Hyper X SSD - Seized	9
SC15	1B23	One (1) Western Digital 1 TB HDD S/N: WCAU45355046 - Seized	10
SC16	1B24	One (1) Western Digital 1 TB HDD S/N: WCAW32328401 - Seized	11
SC17	1B25	One (1) Western Digital 1 TB HDD S/N: WCAU42139599 - Seized	12
SC18	1B26	One (1) Western Digital 1 TB HDD S/N: WCAU45276871 - Seized	13
SC19	1B27	One (1) Samsung 1 TB HDD S/N: S2AEJ18Z408963 - Seized	14
SC20	1B28	One (1) Samsung 1 TB HDD S/N: S2AEJ18Z4408961 - Seized	15
SC21	1B29	One (1) Samsung 1 TB HDD S/N: 52AEJ18Z408962 - Seized	16
SC22	1B30	One (1) 160 GB Western Digital HDD S/N:WMAU2U189169 - Seized	17
SC23	1B31	One (1) 640 GB Western Digital HDD S/N: WCASY0416918 - Seized	18
SC24	1B32	One (1) Western Digital 1 TB HDD S/N: WCAW32653861 - Seized	19
SC25	1B33	One (1) Samsung Phone Model: SPHL710 - Seized	20
SC26	1B34	One (1) HTC Cell Phone S/N: HT068P900155 - Seized	21
SC27	1B35	One (1) Olympus Camera JOH244018 - Seized	n/a
SC28	1B36	One (1) MS ZUHE Mp3 Player S/N: 014195164210 - Seized	n/a

<b>Search Item No.</b>	<b>Evidence No.</b>	<b>Description</b>	<b>Subject Property No.</b>
SC29	1B37	One (1) HTC Phone S/N: HT806G001901 - Seized	22
SC30	1B38	One (1) Garmin NUVI S/N:1C2041768 - Seized	n/a
SC31	1B39	One (1) TP-Link Network USB - Seized	23
SC32	1B40	One (1) SanDisk USB Thumb Drive 16 GB - Seized	24
SC33	1B41	One (1) OSR Thumb Drive - Seized	25
SC34	1B42	One (1) PNY 1 GB Thumb Drive - Seized	26
SC35	1B43	One (1) SanDisk 1 GB Thumb Drive - Seized	27
SC36	1B44	One (1) Sans Thumb Drive - Seized	28
SC37	1B45	One (1) UFCU 128 MB Thumb Drive - Seized	29
SC38	1B46	One (1) 8 GB SanDisk Micro SD - Seized	30
SC39	1B47	One (1) 16 GB Micro SD - Seized	31
SC40	1B48	One (1) ATT Sim Card - Seized	32
SC41	1B49	One (1) bag containing nine (9) Floppy Disks, and five (5) CD/DVD's - Seized	n/a
SC42	1B50	One (1) bag containing fifteen (15) CD/DVD's - Seized	n/a
SC43	1B51	One (1) bag containing twenty-nine (29) CD/DVD's - Seized	n/a
SC44	1B52	One (1) bag containing twenty-eight (28) CD/DVD's - Seized	n/a
SC45	1B53	One (1) bag containing twenty-seven (27) CD/DVD's - Seized	n/a
SC46	1B54	One (1) bag containing seven (7) CD/DVD's - Seized	n/a
SC47	1B55	Black Tower, no serial number	n/a
SC48	1B56	Rack server, no serial number	n/a